

ABSTRACT OF THE DISCLOSURE

A password registration unit encrypts key information using an input password, and stores the generated encrypted key as a file into a computer. A file encryption unit generates  
5 a file key arbitrarily, encrypts the file key using the key information, encrypts a plaintext using the file key to generate a ciphertext, and stores an encrypted file including the encrypted file key in its header part and the ciphertext in its data part. A file decryption unit decrypts the  
10 encrypted file key using the key information to obtain a file key, or receives an input of a password, decrypts the encrypted key using the password to obtain key information, and decrypts the encrypted file key using the key information to obtain a file key. The file decryption unit then decrypts the  
15 ciphertext using the obtained file key.

2006 RELEASE UNDER E.O. 14176